

MSA 9-11-2014

AO 106 (Rev. 04/10) Application for a Search Warrant

Sealed

Public and unofficial staff access
to this instrument are
prohibited by court order.

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

United States Courts
Southern District of Texas
FILED

SEP 11 2014

David J. Bradley, Clerk of Court

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information assoc. with stefano@pcanddexports.com,
alan@pcanddexports.com & alan@alan-industries.com
stored at premises controlled by GoDaddy.com LLC

Case No.

H14-885

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ Arizona _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

**UNSEALED
PER ORDER**

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC 1343, 1344, 1349,
1956(h) and 1957

Offense Description
Wire Fraud; Bank Fraud; Conspiracy to Commit Wire Fraud; Money Laundering
Conspiracy and Monetary Transactions in Property Derived from Specified
Unlawful Activity

The application is based on these facts:
(See facts described in the Affidavit In Support of Search Warrant)

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Kalford Young, Special Agent IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/11/2014

City and state: Houston, Texas

George C. Hanks, Jr.
Judge's signature

George C. Hanks, Jr., U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH
STEFANO@PCANDDEXPORTS.COM;
ALAN@PCANDDEXPORTS.COM
AND ALAN@ALAN-
INDUSTRIES.COM THAT ARE
STORED AT PREMISES
CONTROLLED BY GODADDY.COM
LLC

H14-885

Case No. _____

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Kalford Young, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for an account controlled by the subscription-based web hosting service known as **GoDaddy.com LLC**, headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, Arizona 85260. The accounts to be searched are **stefano@pcanddexports.com**, **alan@pcanddexports.com** and **alan@alan-industries.com** (the “Target Accounts”), which are further described in the following paragraphs and in Attachment A and are located on computers belonging to **GoDaddy.com LLC**. As set forth herein, there is probable cause to believe that on the computer systems of **GoDaddy.com LLC**, there exists evidence, fruits, and

instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1344 (Bank Fraud), and 18 U.S.C. § 1349 (Conspiracy to Engage in a Scheme to Defraud), 18 U.S.C. § 1956(h) (Money Laundering Conspiracy) and 18 U.S.C. § 1957 (monetary transactions in property derived from specified unlawful activity).

2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **GoDaddy.com LLC** to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government authorized persons will review that information to locate items described in Section II of Attachment B.

3. I am a Special Agent with the Internal Revenue Service, Criminal Investigation (IRS-CI), and have been since September 2000. As an IRS-CI Special Agent, my duties include investigating criminal violations of Federal laws, including tax fraud (Title 26), money laundering (18 U.S.C. § 1956) and related violations of Titles 18 and 31. In that capacity, I have conducted and participated in numerous criminal investigations of wire and bank fraud, conspiracy to commit wire or bank fraud, money laundering conspiracy and monetary transactions in

property derived from specified unlawful activity, in violation of 18 U.S.C. §§ 1343, 1344, 1349 and 18 U.S.C. §§ 1956(h) and 1957.

4. The facts set forth in this affidavit are known to me as a result of my personal participation in this investigation and on my conversations with other members of the investigative team and other law enforcement personnel.

5. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that evidence of violations of 18 U.S.C. §1343, 18 U.S.C. § 1344, 18 U.S.C. § 1349, 18 U.S.C. § 1956(h) and §1957 will be found in the Target Accounts.

BACKGROUND REGARDING COMPUTERS, THE INTERNET

AND EMAIL

6. Based on my training, experience, knowledge and discussions with other law enforcement personnel with specialized training and experience, I know the following:

- a. The term “computer” as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any

data storage facility or communications facility directly related to or operating in conjunction with such device.

- b. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web (“www”) is a functionality of the Internet which allows users of the Internet to share information.
- c. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.
- d. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user’s computer, transmitted to the subscriber’s mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may

allow users to post and read messages and to communicate via electronic means.

- e. A domain name is a name that identifies an internet resource such as a website. Domain names are registered in the Domain Name System (DNS), which is a database of network names and internet protocols values (IP) that allows users to find any particular website/address on the internet.
- f. Web hosting is a term for the service of physically maintaining a website and data on a particular computer server and providing a connection to the internet. Web hosting providers are often businesses that rent or lease out space on their servers to customers.

GoDaddy.com LLC

- g. Based on my experience and discussions with other law enforcement personnel with specialized training and experience, I have learned the following about **GoDaddy.com LLC**:
- h. **GoDaddy.com LLC** is a pay for services provider that offers domain registration, web hosting and other related services. Subscribers purchase services from GoDaddy.com LLC via the internet. GoDaddy.com LLC requires subscribers to provide basic contact information, such as name, address, phone number and email address

for billing purposes. GoDaddy.com LLC requires payment for its services and accepts credit cards as a form of payment. GoDaddy.com LLC also collects basic credit card information, such as the account number, name of the cardholder and expiration dates for payments made with a credit card.

- i. Through **GoDaddy.com LLC's** domain name registration service, a subscriber is able to determine whether their desired domain name is available or already in use by someone else. If available, **GoDaddy.com LLC** registers the chosen domain name in the DNS database. The domain registration service can be renewed by the subscriber annually.
- j. **GoDaddy.com LLC** also offers a web hosting service to its subscribers. As part of its web hosting service, **GoDaddy.com LLC** leases a set amount of space on its computer servers to a subscriber. The subscriber stores data or its domain/website on the leased server space that is accessible to the internet. Web hosting is also a service that must be renewed periodically.
- k. In conjunction with its web hosting service, **GoDaddy.com LLC** also offers web based email service to its subscribers. **GoDaddy.com**

LLC provides a set number of mailboxes and storage space that is associated with the subscriber's domain name.

1. **GoDaddy.com LLC** maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. These records include account access information, e-mail transaction information, and account application information.
- m. Subscribers to **GoDaddy.com LLC** may access their accounts on servers maintained and/or owned by **GoDaddy.com LLC** from any computer connected to the Internet located anywhere in the world.
- n. Any e-mail that is sent to a **GoDaddy.com LLC** subscriber is stored in the subscriber's "mail box" on **GoDaddy.com LLC's** servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by **GoDaddy.com LLC**. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on **GoDaddy.com LLC's** servers indefinitely.
- o. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to **GoDaddy.com LLC's** servers, and then transmitted to its end destination. **GoDaddy.com LLC** users have the option of saving a copy of the e-mail sent.

Unless the sender of the e-mail specifically deletes the e-mail from the **GoDaddy.com LLC** server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message, thereby eliminating it from the e-mail box maintained at **GoDaddy.com LLC**, but that message will remain in the recipient's e-mail box unless the recipient deletes it, or unless the recipient's account is subject to account size limitations.

- p. A **GoDaddy.com LLC** subscriber can store files, including e-mails and image files, on servers maintained and/or owned by **GoDaddy.com LLC**.
- q. A subscriber to **GoDaddy.com LLC** may not necessarily store copies on his or her home computer of e-mails and image files stored in his **GoDaddy.com LLC** account. The subscriber may store e-mails and/or other files on the **GoDaddy.com LLC** server for which there is insufficient storage space in the subscriber's computer and/or which he or she does not wish to maintain in the computer in his or her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the **GoDaddy.com LLC** server.

r. Computers located at **GoDaddy.com LLC** contain information and other stored electronic communications belonging to hundreds of thousands of third parties unrelated to this investigation. Accordingly, this affidavit and application for a search warrant seek authorization solely to search the computer account and/or files set forth in Attachment A and following the search procedures described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. See 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

FACTUAL BASIS SUPPORTING PROBABLE CAUSE

8. Crown Financial, LLC is a factoring and hard money lender business located in Houston, TX. Philip Tribe is a member of Crown Financial, LLC. A factoring business purchases accounts receivables from its customers at a discount. The discount percentage is determined by the risk assumed by the factoring company. The factoring business then attempts to collect the debt from the receivable. Businesses typically utilize factoring businesses for cash flow needs.

9. Diversified Business Resources is a financing and factoring company located in Escondido, California.

10. GBL Associates LLC is a corporation based in Colorado. According to the Colorado Secretary of State, GBL Associates LLC was formed in 2013. Its registered agent is Business Filings, Inc. based in Madison, WI. The Manager of the corporation is Bree Davis. According to Bree Davis, GBL Associates LLC is a wholesaler of video game accessories. Bree Davis and Alan Leschyshyn were identified as users of the email account gblassociatesinc@gmail.com

11. PCD Exports LLC is a corporation located at 992 S. 4th Avenue, Suite 100-248, Brighton, CO 80601, according to filings with the Colorado Secretary of State. PCD Exports, LLC is the current name of the corporation; it was previously known as PC&D Exports, LLC. PCD Exports LLC made its initial filing with the Colorado Secretary of State in 2008. According to filings with the Colorado Secretary of State, Alan Leschyshyn caused Articles of Amendment to be filed on February 6, 2013. In addition, on June 18, 2013, Stefano Vitale caused Articles of Amendment to be filed changing the name of PC&D Exports LLC to PCD Exports LLC. Stefano Vitale is also known as Steven Michael Palizzi. Stefano Vitale utilizes several email accounts that have been identified so far during this investigation: svitale@p-conceptsanddesign.com, svitale@me.com, steven.palizzi@me.com and [**stefano@pcanddexports.com**](mailto:stefano@pcanddexports.com).

12. Alan Industries, Inc. is an Arizona corporation. According to the Arizona Corporation Commission, Alan Leschyshyn (Leschyshyn) and his wife Marla Leschyshyn are members of the corporation. The address of the corporation is 3120 West Carefree Highway, Suite 1-659, Phoenix, AZ 85086. Investigation to date has revealed that Leschyshyn utilizes the email accounts aleschys@yahoo.com, bond50@icloud.com, gblassociatesinc@gmail.com, **alan@alan-industries.com** and **alan@pcanddexports.com**. Based on investigation and experience, it is also probable that Leschyshyn utilizes jjgamingincorporated@gmail.com and circle8gaming@gmail.com email accounts. Leschyshyn and Vitale are known associates.

13. JJ Gaming LLC is a Colorado corporation that was incorporated on January 11, 2013 as JJ Gaming Co. Inc. On February 6, 2013, a Combined Statement of Conversion and Articles of Organization were filed by Alan Leschyshyn. On April 23, 2013, Articles of Amendment were filed by Edward Hanania with the Colorado Secretary of State to change the name of the corporation to JJ Gaming LLC. According to the LinkedIn profile of Edward Hanania, he is the Owner and President of JJ Gaming, LLC. He describes the business purpose of JJ Gaming, LLC as, "JJ Gaming is a Wholesale Distribution Company that buys gaming accessories and distribute (sic) them to companies that either sell them, distribute them or bundle them with other products and sell (sic)

them. It is a seasonal business which affords me the time I need to put all of my energy into selling Real Estate.”

14. Premium Concepts & Design Inc. is an Arizona corporation that was incorporated on April 26, 2006. Upon its formation, Vitale (then known as Steven Palizzi) was listed as its sole director. The annual reports filed for Premium Concepts & Design Inc. on August 1, 2012, May 30, 2013 and March 29, 2014 all reflect the character of its business as “Marketing & Promotion for DVD Gaming and Music” and identify Vitale as its sole officer (President), sole director and sole shareholder.

15. EinsteinModz.com is a web site that sells modifications to gaming systems, to include, the XBOX 360 and the Play Station 3. According to the Wisconsin Department of Financial Institutions, EinsteinModz LLC was a Wisconsin corporation located at 3712 Tower Avenue, Suite B, Superior, WI 54880 with Coy Christmas as its registered agent. On April 7, 2014, Wisconsin Department of Financial Institutions filed a Notice of Administrative Dissolution regarding EinsteinModz LLC. EinsteinModz Gaming Group, LLC is incorporated in Delaware. Based on investigation and belief, EinsteinModz LLC became EinsteinModz Gaming Group, LLC. According to an email from gblassociatesinc@gmail.com, BGREM, LLC is the managing company for

EinsteinModz, LLC. BGREM, LLC appears to be incorporated in Delaware as B.G.R.E.M. LLC.

16. In December 2013, Philip Tribe of Crown Financial contacted the FBI regarding a business transaction involving Stefano Vitale. Vitale was attempting to obtain a line of credit in the approximate amount of \$4.3 million. Crown Financial had done a previous business transaction with Vitale. As part of the due diligence process, Crown Financial asked Vitale to provide a personal financial statement (PFS). In response, on December 6, 2013, Vitale using the address **stefano@pcanddexports.com**, sent an email with the subject "Re: To Do List" to Philip Tribe. Attached to the email was a file named *financial statement.pdf*, which was Vitale's personal financial statement. In the PFS, Vitale disclosed that he had a bank account at Wells Fargo Bank with a balance of \$4.2 million. In order to verify the balance, Philip Tribe requested that Vitale provide a copy of his bank statement.

17. On December 12, 2013, Vitale using the address **stefano@pcanddexports.com** sent an email to Philip Tribe with a file named *WF_112013.pdf* attached. The attached file was a bank statement for Vitale's personal Wells Fargo Bank account ending in 3494. According to the statement, the account balance was \$4,208,605.69 and the owner of the account was Stefano G. Vitale. During basic checks to verify the veracity of the bank statement and

other documents, Crown Financial LLC learned that the Wells Fargo Bank statement received from Vitale was fraudulent.

18. Based on the information provided by Crown Financial, the FBI began to investigate Vitale and the individuals and entities associated with Vitale's business dealings with Crown Financial, Vitale's attempt to obtain the line of credit and Crown Financial's previous business transaction with Vitale. Crown Financial LLC provided copies of email correspondence between Crown Financial LLC, Davis, Vitale, Alan Leschyshyn, Tammie Hanania and others. Utilizing these email records, the FBI obtained search warrants for key email accounts. In addition, the FBI also obtained financial and bank account records to review and follow the trail of proceeds through affected accounts.

19. Investigation has revealed that the Wells Fargo Bank statement emailed by Vitale using the address **stefano@pcanddexports.com** to Philip Tribe on December 12, 2013 (as discussed in paragraph 17 above) was fraudulent. Information obtained from Wells Fargo Bank using the same account number as listed on the statement provided by Vitale established that this account was not owned by Vitale and the balance in the account was actually \$0.00.

20. The investigation revealed a scheme to defraud factoring businesses and insurance companies that was replicated and carried out numerous times against different victim companies. The scheme involved numerous individuals

located in multiple jurisdictions with Stefano Vitale and Alan Leschyshyn at its center. Based on a review of email accounts it appears that the scheme has been ongoing since at least 2012. The scheme involves multiple entities controlled by Vitale and Leschyshyn. Vitale and Leschyshyn create false invoices, purchase orders, bank account statements and financial documents in order to document a nonexistent transaction between companies they control. Vitale, Leschyshyn or one of their conspirators contacts factoring businesses to factor the nonexistent accounts receivable. In furtherance of the scheme, and to induce a factoring company to enter into a factoring agreement, the conspirators purchase credit insurance to minimize the risk of collection being assumed by the factoring company. Once the credit insurance and factoring agreement are secured, the fabricated transaction is submitted to the factoring company for payment. After the factoring company purchases the receivable from its customer and funds the transaction, the proceeds are transferred through various entities and accounts and ultimately provided to the various participants in the scheme. The amount payable to the factoring company on the receivable is then not paid causing significant financial losses to the factoring company or the insurance company who provided the credit insurance for the transaction.

Vitale's Prior Transaction with Crown Financial

21. During October 2013, Davis contacted Crown Financial to discuss a factoring arrangement for a transaction between her business, GBL Associates LLC, and PCD Exports LLC. Davis reported to Crown Financial that GBL Associates LLC was trying to sell to PCD Exports LLC 4,011 units of a gaming bundle based on the video game Gears of War. The bundle included a vault that was customized to work with the Gears of War video game. The vault is a shell that is themed with Gears of War which covers the XBOX 360 gaming system.

22. Crown Financial reviewed the information it was provided and determined it was not able to factor the proposed transaction. Instead, Crown Financial agreed to fund GBL Associates LLC's purchase of the gaming bundles from Einsteinmodz.com (its supplier) and upon GBL Associates LLC's collection of payment from PCD Exports LLC (its customer), GBL Associates LLC and Crown Financial would split the profits 50/50 with each receiving approximately \$100,000.

23. As part of the agreement between GBL Associates LLC and Crown Financial, on November 15, 2013, Crown Financial wire transferred \$697,490.84 to BGREM LLC, the manager of EinsteinModz.com LLC.

24. Bank records revealed that immediately after receipt of the wire transfer of \$697,490.84 from Crown Financial on November 15, 2013, the following financial transactions were initiated on November 18, 2013 from the

funds received from Crown Financial: \$610,474.20 was wire transferred from BGREM LLC to Alan Industries LLC; \$512,000.00 was transferred from Alan Industries LLC to Leschyshyn; \$427,000.00 was wire transferred from Leschyshyn to Vitale; and \$85,000.00 was transferred from Leschyshyn to Davis.

25. Bree Davis, the owner of GBL Associates LLC was interviewed on April 3, 2014 by FBI and your affiant. During the interview, Davis admitted that the entire transaction involving Crown Financial was fraudulent. Davis stated that she was coached by Leschyshyn and Vitale on how to apply for the factoring arrangement and what to say deal to the factoring companies. In October 2013, Davis contacted Crown Financial regarding a factoring agreement for transactions between GBL Associates LLC and PCD Exports LLC.

26. Davis admitted to emailing falsified financial statements to Crown Financial in support of her application for factoring and that she emailed a modified bank statement to Crown Financial knowing that the bank statement had been modified. According to Davis, Vitale modified the bank statement to show prior transactions with EinsteinModz.com and PCD Exports LLC that never occurred.

27. Davis also told the agents that according to the deal as presented to Crown Financial, after receiving payment for the transaction, EinsteinModz.com, the supplier, was supposed to ship the goods to PCD Exports LLC's warehouse in

Florida. Davis asked Vitale how the shipment of goods would occur in order to conceal the fraudulent nature of the transaction. Vitale informed Davis that he had everything under control as he had warehouses in Miami and he would move the goods from one warehouse to another in order to simulate that the shipment had occurred.

28. Davis confirmed that after Crown Financial and GBL Associates LLC entered into their agreement, Crown Financial sent \$697,490.84 via wire transfer to BGREM LLC on behalf of GBL Associates LLC; and after receipt, a portion of these funds were then sent from BGREM LLC to Leschyshyn and once received in Leschyshyn's account, Leschyshyn transferred \$85,000 from his account into Davis' account. According to Davis, Rishi Kartaram was involved in the transaction from EinsteinModz.com and was paid \$30,000 for accepting the wire and forwarding the money to Leschyshyn.

Prior Transaction – JJ Gaming LLC

29. Based on a review of bank records and various email accounts, the scheme as outlined above was carried out multiple times by Vitale and Leschyshyn. Each time, a different company was used to obtain credit insurance and obtain the factoring relationship. During 2013, one of the schemes utilized JJ Gaming LLC and Premium Concepts and Design Inc., another corporation owned by Vitale, to obtain factoring and credit insurance.

30. During April 2013, Edward Hanania contacted various factoring companies, including Diversified Business Resources, to apply for a factoring transaction on behalf of JJ Gaming LLC. The receivable they wished to factor was the result of a sale of video game accessories by JJ Gaming LLC to Premium Concepts & Design Inc. JJ Gaming LLC provided DBR with documentation to evidence the sales and resulting receivables, including a sales invoice for \$599,913.81.

31. On April 24, 2013, Vitale sent an email from svitale@me.com to Edward Hanania, at hanania33@yahoo.com with the subject line, "Personal Financial Statement". The text of the email was, "Here is a template..... Fill in some numbers, embellish a bit to make it seem like a better risk, but this is not verified any more than winston did." The attachment, *Financial Statement.xls*, was titled Personal Financial Statement for Edward Hanania, but did not yet contain specific dollar amounts. Based on experience and investigation, the Personal Financial Statement is necessary to determine the credit worthiness of businesses and their owners when applying for factoring of accounts receivable and Vitale is telling Edward Hanania to embellish the financial numbers to make Edward Hanania and his business JJ Gaming LLC appear to be a better risk.

32. On June 13, 2013, an email was forwarded from Leschysyn using the email address aleschys@yahoo.com to jjgamingincorporated@gmail.com. The

subject of this email was "Re: Fwd: Sign and Scan". This email is a chain concerning a file named *QBE.pdf*. This file is an application for trade credit insurance with QBE Insurance Corp. In the initial email, Leschyshyn instructs Edward Hanania to sign and date the document that is attached. The initial file was called *QBE Application for Trade Credit.pdf*. The file *QBE.pdf* was signed by Edward Hanania on June 13, 2013.

33. Based on what it was told and the documentation provided to it by JJ Gaming LLC and Premium Concepts & Design Inc., DBR decided to factor the receivables of JJ Gaming LLC. As part of the deal, JJ Gaming LLC purchased trade credit insurance to insure the credit risk DBR was assuming with the transaction. On August 30, 2013, DBR sent \$479,901.05 to JJ Gaming LLC via a wire transfer.

34. Immediately after receipt of the wire transfer of \$479,901.05 from DBR on August 30, 2013, the following financial transactions were initiated from the funds received from DBR: \$379,901.05 wire transfer from JJ Gaming LLC bank account controlled by Edward Hanania to a JJ Gaming LLC account controlled by Leschyshyn; \$286,300.00 transferred from the JJ Gaming LLC bank account controlled by Leschyshyn to Leschyshyn; \$286,345.00 transfer from Leschyshyn to a bank account of PC&D Exports LLC controlled by Leschyshyn; \$286,301.00 wire transfer from the PC&D Exports LLC bank account controlled

by Leschyshyn to a PC&D Exports LLC account controlled by Vitale; and two (2) transfers totaling \$220,000.00 transferred from PC&D Exports LLC to Vitale.

35. The receivable was due on October 2, 2013. Premium Concepts & Design Inc. did not make any payments on the receivable. After repeated attempts to collect the amounts due from Premium Concepts & Design Inc., DBR and Edward Hanania filed a claim against the trade credit insurance policy purchased by JJ Gaming LLC. During May 2014, QBE Insurance Corp. approved and paid the claim.

36. Based on the investigation to date, the JJ Gaming LLC transaction described above was a fraudulent scheme perpetrated by Vitale, Leschyshyn and Edward Hanania.

37. Prior to the JJ Gaming LLC transaction, on February 14, 2013, Vitale, using the email address Svital@me.com replied to an email from Leschyshyn, utilizing the email address **alan@alan-industries.com**. The subject line of the email was "Re: Colorado" and was the latest in a chain discussion between Vitale and Leschyshyn. In the email, Vitale wrote: "Just one other thing.....You might also want to start finding a factor for JJ Gaming too in the meantime....Same inventory.....Let's talk about pricing per unit before invoices get sent too from both companies....". Based on their previous discussions in the email chain and experience and investigation, Vitale is discussing their furtherance of their ongoing

scheme and discussing the fraudulent JJ Gaming LLC scheme that they eventually perpetrated.

38. Based on a review of bank records and various email accounts, the scheme as outlined above was carried out on multiple occasions by Vitale and Leschyshyn. Each time, they used a different company to obtain credit insurance and obtain the factoring relationship.

Export Import Bank

39. During March 2014, Vitale contacted the Bank of Oklahoma DBA Bank of Arizona to apply for a line of credit for PCD Exports LLC. In concert with the line of credit application, Vitale also applied for a Working Capital Guarantee (WCG) from the Export Import Bank of the United States (ExIm Bank).

40. The WCG is an ExIm Bank program available to small business exporters to provide liquidity by allowing an exporter to obtain advances on their foreign/export related accounts receivables or inventory. For foreign accounts receivable under the WCG program, the exporter obtains a loan or line of credit from a participating lender based on their export related accounts receivables. The ExIm Bank provides the lender with a guarantee for up to 90% of the exporter's foreign/export related accounts receivables. In other words, the ExIm Bank

assumes 90% of the small business exporter's risk of collection from its foreign customers.

41. On March 19, 2014, "Alan Michaels" using the email **alan@pcanddexports.com** sent an email with the subject "Re: Working Capital Guarantee Loan" to David Ridgeway, an employee of Bank of Arizona. The signature line of the email identified "Alan Michaels" as the Chief Financial Officer of PC&D Exports LLC with the email **alan@pcanddexports.com**. Based on the investigation, it is believed "Alan Michaels" is actually Alan Leschyshyn. The investigation revealed that during a previous fraudulent transaction, Leschyshyn requested an email account be established using his middle name "Michael." Attached to the email sent by Leschyshyn to the Bank of Arizona, was a file named *FebBankStatement.pdf*, which was the February 2014 bank statement for Bank of America business account ending 1732 for PC&D Exports LLC. According to the statement provided to Bank of Arizona, the beginning balance of the account on February 1, 2014 was \$783,950.44 and the ending balance on February 28, 2014 was \$2,502.10. The statement also reflected that a total of three (3) transactions occurred within the account, comprised of an incoming wire transfer of \$131,021.24 from JJ Gaming LLC, an incoming wire transfer of \$100,000.00 from Circle 8 Gaming LLC and an outgoing payment of \$1,012,439.58 to American Express. Investigation has revealed that the Bank of

America bank statement emailed by Leschyshyn was fraudulent. Information obtained from Bank of America for the bank account with the same account number as listed on the statement provided by Leschyshyn established that the balance of the account on both February 1, 2014 and February 28, 2014 was actually \$1.00. The statement provided by Bank of America also reflects only two (2) transactions to the account during the month comprised of a credit of \$29.95 transferred in from another account and a monthly service fee debit of \$29.95.

42. On April 15, 2014, Vitale using the address **stefano@pcanddexports.com** sent an email with the subject "Re: PC&D – EXIMBANK Application" to David Ridgeway with carbon copies (cc'd) to **alan@pcanddexports.com** and Fernando Almeida, an employee of the Bank of Oklahoma. A file named *EXIMBANK Application.pdf* was attached to the email. In the email, Vitale wrote "Dave, Attached is the application that you can forward on to Mariella and if there are any errors then I can correct them before I sign it and print it out. Regards, Stefano". The attached file is a completed EXIM Bank application for PCD Exports LLC without signatures. Part C, Certifications, of the application, includes a section titled "Guarantor and Additional Borrower Representations and Certifications." That section asks "Is the Borrower or its Owner now, or ever have been in the past: ... (b) charged with or arrested for any criminal offense other than a minor motor vehicle violation (including offenses

which have been dismissed, discharged, or nolle prosequi)...?” Both boxes applicable to the “Borrower” (i.e. PCD Exports LLC) and “Guarantor” (i.e. Vitale) are checked no. Based on investigation, Vitale was previously known as Steven Michael Palizzi before changing his name to Stefano Guido Vitale. Vitale (then known as Palizzi) was charged with multiple counts of theft and forgery in Adams County, Colorado. On August 7, 2011, Vitale was detained by U.S. Customs in Los Angeles, California and arrested by the Los Angeles Police Department as a fugitive from justice relating to the Adams County, Colorado charges. Vitale was extradited to Colorado. Vitale was convicted of theft greater than \$1,000 and less than \$20,000 and sentenced to two (2) years of probation.

43. During May 2014, a line of credit for \$1 million for PCD Exports LLC was approved by the Bank of Oklahoma DBA Bank of Arizona. On May 5, 2014, Vitale signed a promissory note as Managing Member of PCD Exports LLC and on May 6, 2014, Vitale drew \$900,000.00 from the line of credit. On May 8, 2014, Vitale drew the remaining \$100,000.00 from the line of credit.

44. The Domain Name System (DNS) is a standard technology that manages the names of web sites and other internet domains. The DNS allows users to find any particular website/addresses on the internet based on a database of network names and internet protocol (IP) addresses. Various websites including godaddy.com provide public search capabilities of the DNS registration database.

45. According to a DNS search, the registrar for the domain name **“pcanddexports.com”** is **GoDaddy.com LLC**. The search results also reflect that the domain name **“pcanddexports.com”** was created on June 12, 2013 and last updated on March 14, 2014.

46. According to records obtained from **GoDaddy.com LLC**, the domain name **“pcanddexports.com”** is registered to and billed to Stefano Vitale. **GoDaddy.com LLC** records also reflect that on January 9, 2014, Stefano Vitale purchased the service described as “Email – Business (2GB Total/5 Boxes)” or a one (1) year term, as well as purchased a one (1) year term for “Mini online storage (1GB).”

47. A DNS search reflects that **GoDaddy.com LLC** is also the registrar for the domain name **“alan-industries.com”**. The search results also reflect that the domain name **“alan-industries.com”** was created on April 5, 2012 and last updated on April 1, 2014.

48. According to records obtained from **GoDaddy.com LLC**, the domain name **“alan-industries.com”** is registered and billed to Alan Leschyshyn of Alan Industries LLC. **GoDaddy.com LLC** records also reflect that it provides email service for up to five (5) mailboxes associated with Alan Industries LLC and provides “Mini online storage (1GB)” for the email address **alan@alan-industries.com**. **GoDaddy.com LLC** records also reflect that on April 5, 2014,

Alan Leschyshyn renewed the online storage and email account service for an additional one (1) year period.

49. Based on the foregoing, Affiant submits there is probable cause to believe that the Target Accounts contain fruits, evidence and instrumentalities of violations of and attempted violations of 18 U.S.C. §1343, 18 U.S.C. § 1344, 18 U.S.C. § 1349, 18 U.S.C. § 1956(h), and 18, U.S.C. §1957

SEARCH PROCEDURES

50. In order to facilitate seizure by law enforcement of the computer account and files described in Attachment A, this affidavit and application for search warrant seek authorization to permit employees of **GoDaddy.com LLC** to assist agents in the execution of this warrant. In executing this warrant, the search procedure described in Attachment B will be implemented.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

51. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require **GoDaddy.com LLC** to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

REQUEST FOR SEALING

52. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

AN ORDER PREVENTING GODADDY.COM LLC FROM NOTIFYING THE SUBSCRIBER IS NECESSARY

53. If **GoDaddy.com LLC** is permitted to give notice to the subscriber of the Target Accounts or to any other person of the existence of the Search Warrant, there is reason to believe that the subscriber will destroy evidence of the criminal conduct stored in this e-mail accounts and in other locations and/or cease using the Target Accounts in an attempt to obscure the user's true identity, thereby impeding the criminal investigation. Thus, pursuant to Title 18, United States Code, Section 2705(b), it is respectfully requested that **GoDaddy.com LLC** be ordered not to notify any other person regarding the existence of the search warrant.

CONCLUSION

54. Based on the information above, I submit there is probable cause to believe that on the computer systems owned, maintained and/or operated by **GoDaddy.com LLC** there exists evidence, fruits and instrumentalities of violations of 18 U.S.C. §1343, 18 U.S.C. § 1344, 18 U.S.C. § 1349, 18 U.S.C. §1956(h) and 18 U.S.C. §1957. By this affidavit and application, I request that the Court issue a search warrant directed to **GoDaddy.com LLC**, allowing agents to seize the e-mail and other information stored on **GoDaddy.com LLC** servers for the Target Accounts, and associated files set forth in Attachment A, following the search procedure described in Attachment B.

Respectfully submitted,



Kalford Young
Special Agent
Internal Revenue Service

Subscribed and sworn to before me on September 11, 2014,
2014.



GEORGE C. HANKS, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with stefano@pcanddexports.com; alan@pcanddexports.com and alan@alan-industries.com, including both emails and data files, from the inception of the account until present, which are stored at premises owned, maintained or controlled or operated by **GoDaddy.Com LLC**, a company headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, Arizona 85260.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by GoDaddy.Com LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations and attempted violations of 18 U.S.C. § 1343, 18 U.S.C. § 1344, 18 U.S.C. § 1349, 18 U.S.C. §1956(h) and 18 U.S.C. §1957 involving Stefano Vitale, also known as Steven Palazzi, and/or Alan Leschyshyn including, for each account holder or identifier listed on Attachment A, information pertaining to the following matters:

- 1. All email communications related to Stefano Vitale, also known as Steven Palizzi, Alan Leschyshyn, Bree Davis, Tammie Hanania, Rishi Kartaram and/or Edward Hanania's discussions with co-conspirators;**
- 2. All email communications related to financial and credit transactions, to include but not limited to, bank account records, receipts, bank statements, applications, purchase orders, tax**

return preparation, financial statements, personal income statements, tax forms, contracts or spreadsheets;

- 3. All documents related to financial and credit transactions, to include but not limited to, bank account records, receipts, bank statements, applications, purchase orders, tax return preparation, financial statements, personal income statements, tax forms, contracts or spreadsheets;**
- 4. All email communications with any of the victims in this investigation.**